6. ECUACIONES CUADRÁTICAS

6.1. Ecuación de la forma: $ax^2+bx+c\equiv 0(mód.p)$, con $p\in$ Primo.

1.1 Demostrar que la ecuación $ax^2+bx+c\equiv 0(mód.p)$ tiene solución en la forma $x^2\equiv z(mód.p)$ si, y sólo si $(2a,p)=1$.

Una congruencia cuadrática es una ecuación de la forma $ax^2+bx+c\equiv 0(mód.p)$ donde $a\not\equiv 0(mód.p)$ y p un entero impar primo.
Si $p=2$, se tiene que la congruencia $ax^2+bx+c\equiv 0(mód.p)$, con $mcd(a,2)=1$ es equivalente a una de las formas:

$$x^2\equiv 0(mód.2),\ x^2+1\equiv 0(mód.2),$$
$$x^2+x\equiv 0(mód.2),\ x^2+x+1\equiv 0(mód.2),$$

cuya solución es fácil, ya que el anillo cociente $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$ tiene sólo dos elementos.
Sea p un entero impar donde $mcd(a,p)=1$. Entonces, $mcd(4a^2,p)=1$ y la congruencia cuadrática, con módulo impar resulta:

$$ax^2+bx+c\equiv 0(mód.p)\quad (\mathbf{A})$$

que es equivalente a $4a^2x^2+4abx+4ac\equiv 0(mód.p)$ y que podemos escribir como

$$(2\mathrm{ax}+\mathrm{b})^2\equiv \mathrm{b}^2-4\mathrm{ac}(\mathrm{mód.\,p})$$

Si tenemos en cuenta que $b^2-4ac=d$ es el discriminante de la cuadrática y $(2ax+b)=z$, podemos escribir la ecuación en la forma:

$$z^2\equiv d(mód.p)\quad (\mathbf{B})$$

Si $(\mathbf{A})$ no tiene solución, entonces $(\mathbf{B})$ tampoco.
Si $(\mathbf{B})$ tiene una solución z_1, entonces se tiene que

$$2ax+b\equiv z_1(mód.p)\quad (\mathbf{C})$$

y como $mcd(2a,p)=1$, esta ecuación tiene solución. Luego, $(\mathbf{A})$ también tiene solución por tanto, $(\mathbf{A})$ tendrá solución si, y sólo si $(\mathbf{B})$ también la tiene.
Si la ecuación $(\mathbf{B})$ tiene una solución z_1 entonces una segunda solución z_2 será $p-z_1$, ya que

$$(\mathrm{p}-\mathrm{z}_1)^2\equiv \mathrm{z}_2(\mathrm{mód.\,p})$$

1.2 Resolver la ecuación $x^2-7x+12\equiv 0(mód.13)$.

La ecuación propuesta tiene solución como:

$$\frac{-b\pm\sqrt{b^2-4ac}}{2a}=\frac{7\pm\sqrt{7^2-4*1*12}}{2*1}=\frac{7\pm 1}{2}=\begin{cases}x_1=3\\x_2=4\end{cases}$$

Esta ecuación tiene dos, y sólo dos raíces primitivas enteras: $(3,4)$.

Aunque no es imprescindible es conveniente transformar la ecuación, adaptándola al módulo propuesto, eliminando el coeficiente de *a* y convirtiendo los monomios negativos en positivos. En nuestro caso, $x^2 - 7x + 12 \equiv 0(mód.13)$ es equivalente a

$$\mathrm{x}^2 + 6\mathrm{x} + 12 \equiv 0(\mathrm{mód.}\,13).$$

Para $z^2 \equiv 6^2 - 4 \cdot 1 \cdot 12(mód.13)$, $z^2 \equiv -12(mód.13)$ es equivalente a:

$$\mathrm{z}^2 \equiv 1(\mathrm{mód.}\,13)$$

Si tenemos en cuenta que en la ecuación $x^2 \equiv a(mód.p)$, cuando $a = 1$ ó $a = \alpha^2$, genera soluciones en la forma

$$(\mathrm{p} - \mathrm{a})^2 \equiv \mathrm{a}(\mathrm{mód.}\,\mathrm{p})$$

entonces

$$(13 - 1)^2 \equiv 1(\mathrm{mód.}\,13)$$

donde

$$z_2 = 12 + 13t \text{ y } z_1 \equiv -z_2(mód.13) \equiv 1(mód.13)$$

donde

$$\mathrm{z}_1 = 1 + 13\mathrm{t}.$$

Conocidos los valores de z, las raíces primitivas de x vendrán determinadas por:

$2\mathrm{x} + 6 \equiv 1(mód.13)$, equivalente a $2x \equiv 8(mód.13)$, o sea, $x \equiv 4(mód.13)$.
$2x + 6 \equiv 12(mód.13)$, equivalente a $2x \equiv 6(mód.13)$, o sea, $x \equiv 3(mód.13)$.

La solución a la ecuación planteada es:

$x_1 = 3 + 13t$
$x_2 = 4 + 13t$

Esta ecuación tendrá tantas soluciones como valores se le asignen a *t*, siendo *t* un entero arbitrario.

1.3 Resolver la ecuación $3x^2 + 11x + 1 \equiv 0(mód.7)$.

La ecuación propuesta tiene solución como

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{11 \pm \sqrt{11^2 - 4*3*1}}{2*3} = \frac{-11 \pm \sqrt{109}}{6}$$

Dos, y sólo dos raíces primitivas reales:

$$x_1 = \frac{-11 + \sqrt{109}}{6} \;\; y \;\; x_2 = \frac{-11 - \sqrt{109}}{6}$$

Para resolver $3x^2 + 11x + 1 \equiv 0(mód. 7)$, equivalente a

$$x^2 + 6x + 5 \equiv 0(mód. 7)$$

tenemos que

$$z^2 \equiv 6^2 - 4 \cdot 1 \cdot 5(mód. 5)$$

equivalente a

$$z^2 \equiv 16(mód. 7)$$

y que escribimos como

$$z^2 \equiv 2(mód. 7)$$

admite como soluciones:

$$z_1 = 3 + 7t \text{ y } z_2 = 4 + 7t$$

Conocidos los valores de z, la raíces primitivas de x vendrán determinadas por,

$2x + 6 \equiv 3(mód. 7)$, equivalente a $2x \equiv 4(mód. 7)$, o sea, $x \equiv 2(mód. 7)$
$2x + 6 \equiv 4(mód. 7)$, equivalente a $2x \equiv 5(mód. 7)$, o sea, $x \equiv 6(mód. 7)$

La solución a la ecuación planteada es:

$x_1 = 2 + 7t$
$x_2 = 6 + 7t$

Esta ecuación tendrá tantas soluciones como valores se le asignen a *t.*

1.4 Resolver la ecuación $5x^2 - 3x + 1 \equiv 0(mód. 23)$.

La ecuación propuesta tiene solución como

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{3 \pm \sqrt{(-3)^2 - 4*5*1}}{2*5} = \frac{-3 \pm \sqrt{11i}}{10}$$

Dos, y sólo dos raíces primitivas complejas:

$$x_1 = \frac{-3 + \sqrt{11i}}{10} \quad y \quad x_2 = \frac{-3 - \sqrt{11i}}{10}.$$

$5x^2 - 3x + 1 \equiv 0(mód. 23)$ es equivalente a

$$x^2 + 4x + 14 \equiv 0(mód. 23)$$

Por otra parte, $z^2 \equiv 4^2 - 4 \cdot 1 \cdot 14(mód. 23)$ que es equivalente a

$$z^2 \equiv -40(mód. 23)$$

y que escribimos como

$$z^2 \equiv 6(mód. 23)$$

que admite como soluciones:

$$z_1 = 11 + 23t \text{ y } z_2 = 12 + 23t.$$

Conocidos los valores de *z*, la raíces primitivas de x vendrán determinadas por

$2x + 4 \equiv 11(mód. 23)$, equivalente a $2x \equiv 7(mód. 23)$, o sea, $x \equiv 15(mód. 23)$
$2x + 4 \equiv 12(mód. 23)$, equivalente a $2x \equiv 8(mód. 23)$, o sea, $x \equiv 4(mód. 23)$

La solución a la ecuación planteada es:

$x_1 = 4 + 23t$
$x_2 = 15 + 23t$

Esta ecuación tendrá tantas soluciones como valores se le asignen a *t.*

1.5 Resolver la ecuación $7x^2 - 11x + 130 \equiv (mód. 17)$.

En los supuestos anteriores ha quedado demostrado que, a pesar de las soluciones algebraicas negativas, reales o complejas, las soluciones modulares han sido siempre enteras y positivas. Las primeras generan como máximo dos raíces primitivas, las segundas tendrán tantas soluciones como valores se le asignen al parámetro ***t***.
En la ecuación modular $7x^2 - 11x + 13 \equiv 0(mód. 17)$, si eliminamos el coeficiente a y cambiamos el signo de b, obtenemos una ecuación equivalente a

$$x^2 + 5x + 14 \equiv 0(mód. 17)$$

que hemos conseguido multiplicando los dos miembros de la ecuación por 5 y sacado restos respecto al módulo 17.
Calculamos ahora $z^2 \equiv 5^2 - 4 \cdot 1 \cdot 13(mód. 17)$ que es equivalente a

$$z^2 \equiv -31(mód. 17)$$

y que escribimos como:

$$z^2 \equiv 3(mód. 17)$$

Esta ecuación no admite ninguna solución, ya que ***3*** no es resto cuadrático respecto al módulo 17. Efectivamente, si aplicamos el *Criterio de Euler*

$$a^{(p-1)/2} \equiv \pm 1(mód. p)$$

que en nuestro caso sería

$$3^{(17-1)/2} \equiv -1(mód. 17)$$

La unidad negativa viene a demostrar lo indicado anteriormente. Sin embargo esto no significa que la ecuación modular no tenga solución, de hecho tiene infinitas soluciones para los módulos $19,31,37,43,61,67,71,73, etc.$; basta dar valores a x en la ecuación primitiva y encontrar un número que nos permita, por factorización, un $\mathbb{Z}_n$ para poder utilizarlo como módulo. Por ejemplo, para $x=7$ resulta $279=3^2\cdot 31,$ donde podemos elegir $\mathbb{Z}_{31}$.
El discriminante de $7x^2-11x+13=0$ es igual a $11^2-4\cdot 7\cdot 13=-243$ y la solución de la ecuación es

$$x=\frac{11\pm\sqrt{-243}}{2\cdot 7}=\frac{11\pm 9\sqrt{3}i}{14}$$

dos raíces complejas.
Para la solución de $7x^2-11x+13\equiv 0(mód.31),$ como el $mcd(7,31)=1=7(+9)+31(-2),$ podemos eliminar el coeficiente de a multiplicando la ecuación por *7* y sacando restos respecto al módulo 31, con lo que obtenemos:

$$x^2+25x+24\equiv 0(mód.31),$$

que es equivalente a la anterior.
Ahora debemos buscar un gaussiano $z^2\equiv\Delta(mód.p),$ donde $\Delta=b^2-4ac$ que satisfaga la ecuación

$$2ax+b\equiv z_{1,}z_{2,}(mód.p).$$

Como $z^2\equiv 25^2-4\cdot 24\equiv 529(mód.31)$ es equivalente a $z^2\equiv 2(mód.31)$ y 2 es resto cuadrático de 31, ya que

$$2^{31-1)/2}\equiv 1(mód.31)$$

$z^2\equiv 2(mód.31)$ tiene como solución $z\equiv 8,23(mód.31)$

Para $2x+25\equiv 8(mód.31)$ la solución es $x\equiv 7(mód.31)$
Para $2x+25\equiv 23(mód.31)$ la solución es $x\equiv 30(mód.31)$

La solución a la ecuación $7x^2-11x+13\equiv 0(mód.31)$ resulta $x\equiv 7,30(mód.31).$

6.2. Ecuación de la forma: $ax^2+bx+c\equiv 0(mód.m),$ con m compuesto.

2.1 Resolver la ecuación $4x^2+3x-10\equiv 0(mód.35).$

La ecuación $4x^2+3x-10\equiv 0(mód.35)$ que es equivalente a

$$x^2+27x+15\equiv 0(mód.35)$$

tendrá solución si, y sólo si a su vez la tienen:

$$x^2+27x+15\equiv 0(mód.5) \text{ y } x^2+27x+15\equiv 0(mód.7)$$

La primera ecuación, equivalente a $x^2+2x\equiv 0(mód.5)$, tiene como soluciones x_1=0+5t y x_2=3+5t. En cuanto a la segunda, equivalente a $x^2+6x+1\equiv 0(mód.7)$, x_1=3+7t y x_2=5+7t son sus dos raíces.
Para calcular las raíces de la ecuación planteada, que en este caso serán cuatro, utilizaremos el *Teorema Chino de Restos*.

$$0+5t\equiv 3(mód.7) \text{ es equivalente a } 5t\equiv 3(mód.7), \text{ o sea, } t\equiv 2(mód.7)$$
$$0+5t\equiv 3(mód.7) \text{ es equivalente a } 5t\equiv 5(mód.7), \text{ o sea, } t\equiv 1(mód.7)$$
$$3+5t\equiv 3(mód.7) \text{ es equivalente a } 5t\equiv 0(mód.7), \text{ o sea, } t\equiv 0(mód.7)$$
$$3+5t\equiv 5(mód.7) \text{ es equivalente a } 5t\equiv 2(mód.7), \text{ o sea, } t\equiv 6(mód.7)$$

Ahora, despejamos los valores de las distintas x como sigue:

$$x=0+5(2+7t)=10+35t,\quad x=0+5(1+7t)=5+35t$$
$$x=3+5(0+7t)=3+35t,\quad x=3+5(6+7t)=33+35t$$

por tanto las soluciones a la ecuación serán:

$$x\equiv 3,5,10,33(mód.35)$$

2.2 Resolver la ecuación $7x^2-11x+4\equiv 0\left(mód.65\right)..$

La ecuación $7x^2-11x+4\equiv 0(mód.65)$, equivalente a $x^2+17x+47\equiv 0(mód.65)$, tendrá solución si, y sólo si, a su vez la tienen:

$$x^2+17x+47\equiv 0(mód.5) \text{ y } x^2+17x+47\equiv 0(mód.13)$$

La primera, equivalente a $x^2+2x+2\equiv 0(mód.5)$, tiene como soluciones x_1=1+5t y x_2=2+5t. En cuanto a la segunda, equivalente a $x^2+4x+8\equiv 0(mód.13)$, x_1=1+13t y x_2=8+13t son sus dos raíces.
Como en el supuesto anterior, aplicando el *Teorema Chino de Restos* obtenemos las cuatro raíces que son:

$$x\equiv 1,21,27,47(mód.65)$$

2.3 Resolver la ecuación $x^2+96x+113\equiv 0(mód.119).$

La factorización del módulo es $119=7\cdot 17$. Luego, la ecuación tendrá solución si a su vez la tiene con los módulos *7* y 17.
Para $x^2+96x+113\equiv 0(mód.7)$ que simplificada es $x^2+5x+1\equiv 0(mód.7)$, admite la unidad como única solución, esto es, $x=1+7t$.
En cuanto a $x^2+96x+113\equiv 0(mód.17)$, equivalente a $x^2+11x+11\equiv 0(mód.17)$, resulta que

$$z^2\equiv 11^2-4\cdot 11(mód.17)$$

esto es

$$z\equiv 3,14(mód.17)$$

Si ahora resolvemos la ecuación $2x + 11 \equiv 3{,}14(mód. 17)$, obtenemos:

$$x_1 = 10 + 17t \text{ y } x_2 = 13 + 17t$$

que son sus raíces.
La solución a la ecuación propuesta, es:

$$x \equiv 64{,}78(mód. 119)$$

2.4 Resolver la ecuación $x^2 + x + 1 \equiv 0(mód. 1729)$.

Los factores primos del módulo son $1729 = 7 \cdot 13 \cdot 19$, la ecuación tendrá solución si a su vez la tiene con todos y cada uno sus factores.
Operando como en supuestos anteriores, obtenemos:

$$x \equiv 2{,}4(mód.7),\ x \equiv 3{,}9(mód.13) \text{ y } x \equiv 7{,}11(mód.19)$$

Aplicando el *Teorema Chino de Restos*, las soluciones a la ecuación planteada son:

$$x \equiv 562{,}653{,}809{,}828{,}900{,}919{,}1075{,}1166(mód.1729)$$

2.5 Resolver la ecuación $x^2 + 3x - 1 \equiv 0(mód. 4089)$.

Tenemos que $4089 = 3 \cdot 29 \cdot 47$ y ahora probamos si estos factores tienen solución a la ecuación propuesta.
Como en los supuestos anteriores, resulta para los dos primeros:

$$x \equiv 1{,}2(mód.3) \text{ y } x \equiv 8{,}18(mód.29)$$

Para la ecuación $x^2 + 3x - 1 \equiv 0(mód. 47)$ no existe solución y lo probamos:
Tenemos

$$z^2 \equiv b^2 - 4ac(mód. p)$$

esto es

$$z^2 \equiv 13(mód. 29)$$

Si aplicamos el criterio de Euler

$$13^{(47-1)/2} \equiv -1(mód. 47)$$

genera como solución la unidad negativa, lo que significa que 13 no es resto cuadrático respecto al módulo 47. Si z no tiene solución, tampoco la tendrá $2x + 3 \equiv z(mód. 47)$ luego

$$x^2 + 3x - 1 \not\equiv 0(mód. 47)$$

y por tanto, tampoco tendrá solución la ecuación planteada, esto es:

$$x^2 + 3x - 1 \not\equiv 0(mód. 4089)$$

6.3. Ecuación de la forma: $ax^2+bx+c\equiv 0(mód.p^n),$ con $n>1.$

3.1 Resolver la ecuación $x^2+1\equiv 0\left(mód.25\right).$

Estamos ante una congruencia de la forma

$$f(x)\equiv 0(mód.p^a)$$

que se reduce a su equivalente

$$f(x)\equiv 0(mód.p)$$

y que tiene como solución:

$$x\equiv x_1(mód.p)$$

Como $25=5^2=5\cdot 5,$ la ecuación planteada tendrá solución si, y sólo si la tiene

$$x^2+1\equiv 0(mód.5)$$

Del sistema completo de restos respecto a 5, {0, 1, 2, 3, 4}, satisfacen a la ecuación el *2* y el *3*, que podemos escribir como $x=2+5t$ y $x=3+5t.$ Si damos valores a ***t*,** las soluciones menores a 25 que satisfacen al módulo *5* son, 7, 12, 17, 22, 8, 13, 18 y 23 de las que al menos dos deberían satisfacer al módulo *25*. Probando con todas ellas satisfacen la ecuación el 7 y el 18, luego $x\equiv 7,18(mód.25)$ es la solución buscada.

El planteamiento anterior incrementa su dificultad a medida que aumenta la base del exponente, habida cuenta de la cantidad de operaciones a realizar. Para evitar esta situación podemos utilizar la *Fórmula de Taylor* de tal forma que toda solución $x\equiv x_1(mód.p)$ de la congruencia $f(x)\equiv 0(mód.p)$ y con la condición de que la derivada $f'(x_1)$ no sea divisible por *p*, proporciona una solución de la congruencia $f(x)\equiv 0(mód.p^a)$ en la forma $x\equiv x_\alpha(mód.p^\alpha)$ que es equivalente a $x=x_\alpha+p^\alpha t_\alpha.$

Sabemos que $x^2+1\equiv 0(mód.5)$ tiene como soluciones $x=2+5t$ y $x=3+5t.$ Para $f(x)$:

$$f(2)=x^2+1=5 \text{ y } f(3)=x^2+1=10$$

y para la derivada $f'(x)=2x,$ los valores serán:

$$f'(2)=2x=4 \text{ y } f'(3)=2x=6$$

donde, ni el *4* ni el *6* son divisibles por *25*, por lo que no es necesario recurrir a la segunda derivada. Primero resolvemos

$$f(2)+5t_1 f'(2)\equiv 0(mód.25)$$

que es equivalente a

$$5+5t_1\cdot 4\equiv 0(mód.25)$$

esto es

$$5+20t_1 \equiv 0(mód.25)$$

Dividiendo por *5* y haciendo operaciones, $t_1 \equiv 1(mód.5)$ y equivalente a $t_1 = 1+5t$. Ahora

$$x = 2+5(1+5t) = 7+25t$$

o sea

$$x = 7+25t$$

Resolvemos $f(3)+5t_1 f'(3) \equiv 0(mód.25)$ equivalente a $10+5t_1 \cdot 6 \equiv 0(mód.25)$. Dividiendo por 5 y haciendo operaciones, $t_1 \equiv 3(mód.5)$ que representamos como $t_1 \equiv 3+5t$.
Por el *Teorema Chino de Restos*

$$x = 3+5(3+5t) = 18+25t$$

resulta

$$x = 18+25t.$$

Las solución al sistema planteado es

$$x \equiv 7,18(mód.25)$$

igual al obtenido anteriormente.

3.2 Resolver la ecuación $5x^2 + 13x + 1 \equiv 0(mód.\ 17^2)$.

La ecuación $5x^2 + 13x + 1 \equiv 0(mód.\ 17^2)$ tendrá solución si y sólo si la tiene:

$$5x^2 + 13x + 1 \equiv 0(mód.\ 17)$$

Para $5x^2 + 13x + 1 \equiv 0(mód.\ 17)$ las soluciones son:

$$x_1 = 3 + 17t \text{ y } x_2 = 8 + 17t$$

Los valores de estas raíces, para la ecuación y su derivada, son:

$$f_{(x)} = 5x^2+13x+1 \begin{cases} f_{(3)} = 85 \\ f_{(8)} = 425 \end{cases} \text{ y } f'_{(x)} = 10x+13 \begin{cases} f'_{(3)} = 43 \\ f'_{(8)} = 93 \end{cases}$$

Aplicando estos valores a la ecuación $f(x)+f'(x)\cdot p \cdot t_1 \equiv 0(mód.p^n)$, resulta:

$$85+43\cdot 17t \equiv 0(mód.17^2)$$

que dividido por 17 obtenemos $5+43t \equiv 0(mód.17)$.
Despejando *t*, $t \equiv 7(mód.17)$ resulta para x:

$$x = 3 + 17(7 + 17t) = 122 + 17t^2$$

Ahora

$$425 + 93 \cdot 17t \equiv 0(mód.17^2)$$

que divido por 17, $25 + 93t \equiv 0(mód.17)$.
Despejando *t*, $t \equiv 16(mód.17)$. Luego para x resulta:

$$x = 8 + 17(16 + 17t) = 280 + 17t^2.$$

Las soluciones a la ecuación propuesta, son:

$$x \equiv 122,280(mód.17^2)$$

3.3 Resolver la ecuación $x^2 + 3x + 2 \equiv 0(mód. 245)$.

La factorización del módulo es $245 = 5 \cdot 7^2$ luego la ecuación tendrá solución si, y sólo si también tiene solución con los módulos *5, 7* y *49*.

Para $x^2 + 3x + 2 \equiv 0(mód. 5)$ las soluciones son, $x_1 = 3 + 5t$ y $x_2 = 4 + 5t$
Para $x^2 + 3x + 2 \equiv 0(mód. 7)$ las soluciones son, $x_1 = 5 + 7t$ y $x_2 = 6 + 7t$

Los valores de estas últimas raíces, para la ecuación y su derivada, son:

$$f_{(x)} = x^2 + 3x + 2 \begin{cases} f_{(5)} = 42 \\ f_{(6)} = 56 \end{cases} \text{ y } f'_{(x)} = 2x + 3 \begin{cases} f'_{(5)} = 13 \\ f'_{(6)} = 15 \end{cases}$$

Aplicando estos valores a la ecuación $f(x) + f'(x) \cdot p \cdot t_1 \equiv 0(mód.p^n)$ resulta:

$$42 + 13 \cdot 7t \equiv 0(mód.7^2)$$

que dividido por 7 obtenemos:

$$6 + 13t \equiv 0(mód.7)$$

Despejando *t*, $t \equiv 6(mód.7)$. Ahora x resulta:

$$x = 5 + 7(6 + 7t) = 47 + 7^2 t$$

Por el mismo procedimiento obtenemos la segunda raíz:

$$x = 48 + 7^2 t$$

Tenemos por una parte

$$x_1 = 3 + 5t \text{ y } x_2 = 4 + 5t$$

y por otra

$x_1 = 47 + 7^2t$ y $x_2 = 48 + 7^2t$

que generan cuatro raíces para $x^2 + 3x + 2 \equiv 0(mód. 245)$.
Por el *Teorema Chino de Restos*, obtenemos:

$3 + 5t \equiv 47(mód. 7^2), 5t \equiv 44(mód. 7^2, t \equiv 48(mód. 7^2)$
$x = 3 + 5(48 + 7^2t) = 243 + 7^2t$

$3 + 5t \equiv 48(mód. 7^2), 5t \equiv 45(mód. 7^2, t \equiv 9(mód. 7^2)$
$x = 3 + 5(9 + 7^2t) = 48 + 7^2t$

$4 + 5t \equiv 47(mód. 7^2), 5t \equiv 43(mód. 7^2, t \equiv 38(mód. 7^2)$
$x = 4 + 5(38 + 7^2t) = 194 + 7^2t$

$3 + 5t \equiv 48(mód. 7^2), 5t \equiv 44(mód. 7^2, t \equiv 48(mód. 7^2)$
$x = 4 + 5(48 + 7^2t) = 244 + 7^2t$

Luego, las soluciones a la ecuación propuesta son:

$x \equiv 48,194,243,244(mód.245)$

3.4 Resolver la ecuación $3x^2 + 2x + 10 \equiv 0(mód. 3971)$.

La factorización del módulo es, $3971 = 11 \cdot 19^2$ luego, la ecuación tendrá solución si, y sólo si también tiene solución con los módulos *11, 19* y *361*.

Para $3x^2 + 2x + 10 \equiv 0(mód. 11)$ las soluciones son:

$x_1 = 4 + 11t$ y $x_2 = 10 + 11t$

Para $3x^2 + 2x + 10 \equiv 0(mód. 19)$ las soluciones son:

$x_1 = 5 + 19$ y $x_2 = 7 + 19t$

Los valores de estas últimas raíces, para la ecuación y su derivada, son:

$$f_{(x)} = 3x^2 + 2x + 10 \begin{cases} f_{(5)} = 95 \\ f_{(7)} = 171 \end{cases} \text{ y } f'_{(x)} = 6x + 2 \begin{cases} f'_{(5)} = 32 \\ f'_{(7)} = 44 \end{cases}$$

Si aplicamos el mismo procedimiento que en el supuesto anterior, obtendremos:

$x \equiv 81,1242,2325,2969(mód.3971)$.

3.5 Resolver la ecuación $x^2 + 7x + 5 \equiv 0(mód. 1333241)$.

La factorización del módulo es $1333241 = 7^3 \cdot 13^2 \cdot 23$. La ecuación planteada tendrá solución si, y sólo si admite soluciones con todos y cada uno de los módulos que conforman la factorización, esto es $7, 7^2, 7^3, 13, 13^2$ y 23.

Para $x^2 + 7x + 5 \equiv 0\ (mód. 23)$, las raíces son:

$$x_1 = 2 + 23t \; y \; x_2 = 14 + 23t$$

Para $x^2 + 7x + 5 \equiv 0 \; (mód. 13)$, las raíces son:

$$x_1 = 1 + 13t \; y \; x_2 = 5 + 13t$$

Para la solución de $x^2 + 7x + 5 \equiv 0 \; (mód. 13^2)$ necesitamos conocer los valores numéricos de la ecuación $x^2 + 7x + 5 \equiv 0 \; (mód. 13)$ y su derivada, que son:

$$f_{(x)} = x^2 + 7x + 5 \begin{cases} f_{(1)} = 13 \\ f_{(5)} = 65 \end{cases} \text{ y } f'_{(x)} = 2x + 7 \begin{cases} f'_{(1)} = 9 \\ f'_{(5)} = 17 \end{cases}$$

Ahora utilizamos la ecuación $f(x) + f'(x) \cdot p \cdot t_1 \equiv 0 (mód. p^n)$ o $f(13) + f'(9) \cdot 13t \equiv 0 (mód. 13^2)$, que dividida por 13 resulta:

$$1 + 9t \equiv 0 (mód. 13)$$

de donde

$$t \equiv 10 (mód. 13)$$

Finalmente calculamos

$$x = 1 + 13(10 + 13t) = 131 + 13^2 t$$

esto es

$$x = 131 + 13^2 t$$

Para calcular a segunda raíz de $x^2 + 7x + 5 \equiv 0 \; (mód. 13^2)$ utilizamos los valores numéricos de $x_2 = 5 + 13t$, que son:

$$f(65) + f'(17) \cdot 13t \equiv 0 (mód. 13^2)$$

que dividida por 13 resulta:

$$5 + 17t \equiv 0 (mód. 13^2)$$

de donde, $t \equiv 2 (mód. 13)$ y $x = 5 + 13(2 + 13t) = 31 + 13^2 t$, esto es:

$$x = 31 + 13^2 t$$

Las raíces de $x^2 + 7x + 5 \equiv 0 \; (mód. 13^2)$ son:

$$x_1 = 31 + 13^2 \, t \; y \; x_2 = 131 + 13^2 t$$

La ecuación $x^2 + 7x + 5 \equiv 0 \; (mód. 7)$ tiene como raíces:

$$x_1 = 3 + 7t \; y \; x_2 = 4 + 7t$$

Para resolver $x^2 + 7x + 5 \equiv 0\ (mód. 7^2)$, los valores numéricos son,:

$$f_{(x)} = x^2 + 7x + 5 \begin{cases} f_{(3)} = 35 \\ f_{(4)} = 49 \end{cases} \text{ y } f'_{(x)} = 2x + 7 \begin{cases} f'_{(3)} = 13 \\ f'_{(4)} = 15 \end{cases}$$

Aplicando estos valores a la ecuación $f(x) + f'(x) \cdot p \cdot t_1 \equiv 0(mód. p^n)$ obtenemos para el módulo 7^2:

$$x = 3 + 7(5 + 7t) = 38 + 7^2 t, \text{ y } x = 4 + 7(0 + 7t) = 4 + 7^2 t.$$

Para la ecuación $x^2 + 7x + 5 \equiv 0\ (mód. 7^3)$, los valores numéricos, son:

$$f_{(x)} = x^2 + 7x + 5 \begin{cases} f_{(4)} = 49 \\ f_{(38)} = 1715 \end{cases} \text{ y } f'_{(x)} = 2x + 7 \begin{cases} f'_{(4)} = 15 \\ f'_{(38)} = 83 \end{cases}$$

La ecuación $f(49) + f'(15) \cdot 7^2 t \equiv 0(mód. 7^3)$ dividida por 7^3 resulta:

$$1 + 15t \equiv 0(mód. 7)$$

que genera la raíz

$$x = 4 + 7^2(6 + 7t) = 298 + 7^3 t$$

esto es

$$x = 298 + 7^3 t$$

Para $f(1715) + f'(83) \cdot 7^2 t \equiv 0(mód. 7^3)$, dividida por 7^2 es:

$$35 + 83t \equiv 0(mód. 7)$$

genera la segunda raíz

$$x = 38 + 7^2(0 + 7t) = 38 + 7^3 t$$

esto es

$$x = 38 + 7^3 t$$

La ecuación $x^2 + 7x + 5 \equiv 0\ (mód. 7^3)$ tiene como raíces,

$$x_1 = 38 + 7^3 t \; y \; x_2 = 298 + 7^2 t.$$

Utilizando el *Teorema Chino de Restos*, resulta:

$$\text{x} \equiv 74729,364564,440107,603292,729942,893127,968670,1258505(\text{mód. } 1333241)$$

Son las soluciones a la ecuación $x^2 + 7x + 5 \equiv 0(mód. 1333241)$.

6.4. Ecuación de la forma: $ax^{\varphi(p)+2}+bx^{\varphi(p)+1}+c\equiv 0(mód.p)$, con $p\in$ Primo.

4.1 Resolver la ecuación $x^8+6x^7+1\equiv 0(mód.7)$.

Conocemos ya que $\varphi(n)$ es la función de Euler y que para n primo, $\varphi(n)=p-1$. En nuestro caso, $\varphi(7)$=7-1=6.
Como

$$x^8=x^{\varphi(7)+2=6+2} \text{ y } x^7=x^{\varphi(7)+1=6+1}$$

la ecuación propuesta tiene solución ya que el exponente de $ax^n\ y\ de\ bx^n$ son múltiplos de $n=\varphi(p)+2$ y $n=\varphi(p)+1$, respectivamente. Si no fueran múltiplos, la ecuación podría tener otras soluciones, pero no serían cuadráticas.
La ecuación $x^2+6x+1\equiv 0(mód.7)$, tiene como soluciones:

$$x\equiv 3{,}5(mód.7)$$

La ecuación $x^8+6x^7+1\equiv 0(mód.7)$, también tiene como soluciones:

$$x\equiv 3{,}5(mód.7)$$

pero también tienen la misma solución:

$$x^8+6x+1\equiv 0(mód.7) \text{ y } x^2+6x^7+1\equiv 0(mód.7)$$

Las posibilidades son que las raíces primitivas

x_1 =3+7t ó x_2 =5+7t

al ser paramétricas e independientes, alcanzan una dimensión no sólo por los valores asignados a *t*, sino por los valores asignados al múltiplo de $\varphi(p)+2$ y/o a $\varphi(p)+1$, que convierten estas ecuaciones en unos sistemas numéricos multidimensionales de soluciones infinitas.

4.2 Resolver la ecuación $4x^{10}+10x-1\equiv 0(\text{mód.}5)$.

Empecemos por transformar la ecuación en $x^2+1\equiv 0(mód.5)$ que es equivalente a la propuesta. Esta ecuación tiene como soluciones $x\equiv 2{,}3(mód.5)$.
Como $2^{\varphi(5)+2}=2\cdot 4+2=10$, la ecuación propuesta tendrá dos raíces básicas

x_1 =2+5t y x_2 =3+5t

generando un sistema de infinitas soluciones.

4.3 Resolver la ecuación $x^{26}+7x^{13}+6\equiv 0(mód.13)$.

La ecuación planteada es equivalente a $x^2+7x+6\equiv 0(mód.13)$ que tiene como soluciones

$$x\equiv 7{,}12(mód.13)$$

Teniendo en cuenta que $\varphi(13)=13-1=12$, claramente se observa que $26=2\cdot 12+2$ y $13=12+1$, luego $x\equiv 7{,}12(mód.13)$ tiene como raíces básicas:

x_1 =7+13t y x_2 =12+13t

4.4 Resolver la ecuación $5x^2 + 6x^{33} + 7 \equiv 0(mód. 17)$.

Transformamos la ecuación a su equivalente $x^2 + 8x + 15 \equiv 0(mód. 17)$ cuyas soluciones son:

$$x \equiv 12,14(mód. 17)$$

Observamos que el exponente modificado es el de bx

$$2\varphi(17) = 2(17-1) + 1 = 33$$

por lo que las raíces básicas de $x^2 + 8x^{33} + 15 \equiv 0(mód. 17)$ son:

x_1 =12+17t y x_2 =14+17t

4.5 Resolver la ecuación $x^{182} + 13x^{181} + 23 \equiv 0(mód. 19)$.

Como

$$\varphi(19) = 19 - 1 = 18$$

de donde

$$182 = 10 \cdot 18 + 2$$

o bien

$$181 = 10 \cdot 18 + 1$$

la ecuación equivalente es

$$x^2 + 13x + 23 \equiv 0(mód.19)$$

que tiene como raíces básicas:

$$x \equiv 12,13(mód.19)$$

que a su vez, satisfacen a la ecuación planteada.

6.5. Ecuación de la forma: $ax^{\varphi(p)+2} + bx^{\varphi(p)+1} + c \equiv 0(mód.m)$, **con** m **compuesto.**

5.1 Resolver la ecuación $x^{14} + 3x^{13} - 4 \equiv 0(mód. 21)$.

La factorización del módulo es $21 = 3 \cdot 7$ y $\phi(21) = 3 \cdot 7(\frac{2}{3} \cdot \frac{6}{7}) = 12$.

Como

$$x^{12+2=14} + 3x^{12+1=13} - 4 \equiv 0(mód.21)$$

la ecuación planteada tiene solución.

La ecuación $x^2+3x-4\equiv 0(mód.3)$ tiene como soluciones:

$$x_1=1+3t \text{ y } x_2=2+3t$$

La ecuación $x^2+3x-4\equiv 0(mód.7)$ tiene como soluciones:

$$x_1=1+7t \text{ y } x_2=3+7t$$

La ecuación $x^2+3x-4\equiv 0(mód.21)$ tiene como soluciones:

$$x_1=1+21t, x_2=8+21t$$

luego

$$x_3=10+21t \text{ y } x_4=17+21t$$

La solución básica a la ecuación planteada es:

$$x^{14}+3x^{13}-4\equiv 1,8,10,17(mód.21)$$

5.2 Resolver la ecuación $11x^{50}+13x+17\equiv 0(mód.35)$.

La factorización del módulo es $35=5\cdot 7$ y $\phi(35)=5\cdot 7(\frac{4}{5}\cdot\frac{6}{7})=24$. Como $50=2\cdot 24+2$, la ecuación planteada tiene solución.

Para $11x^2+13x+17\equiv 0(mód.5)$, tenemos como solución:

$$x_1=3+5t \text{ y } x_2=4+5t$$

Para $11x^2+13x+17\equiv 0(mód.7)$ tenemos como solución:

$$x_1=4+7t \text{ y } x_2=5+7t$$

Utilizando el *Teorema Chino de Restos*, obtenemos:

$$x\equiv 4,18,19,33(mód.35)$$

como soluciones base de la ecuación propuesta.

5.3 Resolver la ecuación $x^{34}+17x^{33}+19\equiv 0(mód.51)$.

La función Euler $\phi(51)=3\cdot 17(\frac{2}{3}\cdot\frac{16}{17})=32$. Los exponentes son $34=32+2$ y $33=32+1$ luego, la ecuación planteada tiene solución.
La ecuación es equivalente a $x^2+17x+19\equiv 0(mód.51)$.

Si $x^2+17x+19\equiv 0(mód.3)$ tiene como solución:

$$x = 2 + 5t$$

Si $x^2 + 17x + 19 \equiv 0(mód.17)$ tiene como solución:

$$x_1 = 7 + 17t \text{ y } x_2 = 10 + 17t$$

Utilizando el *Teorema Chino de Restos*, obtenemos:

$$x \equiv 41,44(mód.51)$$

que son las soluciones base de la ecuación planteada.

5.4 Resolver la ecuación $x^{146} + 5x^{49} - 11 \equiv 0(mód.65)$.

La solución a la ecuación $x^2 + 5x - 11 \equiv 0(mód.5)$ es:

$$x \equiv 1,4(mód.5)$$

y la solución a la ecuación $x^2 + 5x - 11 \equiv 0(mód.13)$ es:

$$x \equiv 3,5(mód.13)$$

luego, utilizando el *Teorema Chino de Restos*, la solución a la ecuación

$$x^2 + 5x - 11 \equiv 0(mód.65)$$

es

$$x \equiv 16,29,31,44(mód.65)$$

Como la función Euler tiene como resultado

$$\phi(65) = 5 \cdot 13(\tfrac{4}{5} \cdot \tfrac{12}{13}) = 48$$

y la descomposición de los exponentes

$$146 = 3 \cdot 48 + 2 \text{ y } 49 = 48 + 1$$

la solución anterior es también solución de la ecuación planteada.

5.5 Resolver la ecuación $x^{122} + 4x^{181} - 5 \equiv 0(mód.77)$.

Como $\varphi(77) = 60$, aplicando métodos anteriores, obtenemos las siguiente solución:

$$x \equiv 1,23,50,72(mód.77)$$

6.6. Ecuación de la forma: $ax^{\varphi(p)+2}+bx^{\varphi(p)+1}+c\equiv 0(mód.p^n)$, con $n>1$.

6.1 Resolver la ecuación $x^{22}+x^{21}+3\equiv 0(mód.25)$.

La *función Euler* tiene como solución:

$$\varphi(p^\alpha)=p^\alpha-\ p^{\alpha-1}=5^2-5=20$$

Como $22=20+2$ y $21=20+1$, la solución de la ecuación propuesta, si la tiene, será solución como cuadrática.

Para $x^2+x+3\equiv 0(mód.5)$, tenemos como solución:

$$x_1=1+5t\ y\ x_2=3+5t$$

Para $x^2+x+3\equiv 0(mód.5^2)$, tenemos como solución:

$$x_1=8+5^2t\ y\ x_2=16+5^2t$$

Esta solución también es la de la ecuación propuesta, o sea:

$$x\equiv 8,16(mód.5^2)$$

6.2 Resolver la ecuación $x^{86}-x^{43}-2\equiv\ 0(mód.49)$.

Para el módulo *49*, la *función Euler* da como resultado *42* y $86=2\cdot 42+2$ ó $43=42+1$.

Para $x^2-x+2\equiv 0(mód.7)$, tenemos como solución:

$$x_1=2+7t\ y\ x_2=6+7t$$

Para $x^2-x+2\equiv 0(mód.7^2)$, tenemos como solución:

$$x_1=2+7^2t\ y\ x_2=48+7^2t$$

Solución que también satisface a la ecuación propuesta.

6.3 Resolver la ecuación $x^{296}+2x^{295}+1\equiv\ 0(mód.343)$.

La factorización del módulo es $343=7^3$ y la *función Euler*

$$\varphi(7^3)=7^3-7^2=294$$

que se ajusta a los exponentes de la ecuación planteada.

La ecuación $x^2+2x+1\equiv 0(mód.7)$, tiene como solución:

$$x\equiv 6(mód.7)$$

La solución con módulo 7^3:

$$x \equiv 48,97,146,195,244,293,342(mód.7^3)$$

La solución anterior es la de la ecuación presentada, ya que es la solución base.

6.4 Resolver la ecuación $x^{164} - 2x^{163} + 1 \equiv 0(mód.\ 3^5)$.

La ecuación $x^2 - 2x + 1 \equiv 0(mód.\ 3)$ admite la solución de $x \equiv 1(mód.\ 3)$.

Para el módulo 3^5 admite:

$$x \equiv 1,28,55,82,109,136,163,190,217(mód.3^5)$$

Es la solución base de esta ecuación.

6.5 Resolver la ecuación $2x^2 + 3x + 1 \equiv 0(mód.28)$ y calcular exponentes ≤ 150.

La ecuación admite como solución

$$x \equiv 3,27(mód.\ 28)$$

que son las raíces base.

La *función Euler* $\varphi(28) = 12$ luego, los exponentes ≤ 150 que admitirán serán:

Para $2x^n$: $n = 2,14,26,38,50,62,74,86,98,110,122,134,146$
Para $3x^n$: $n = 1,13,25,37,49,61,73,85,97,109,121,133,145$

6.7. Ecuación cuadrática a partir de un número dado.

7.1.Procedimientos para generar una ecuación cuadrática.

En una ecuación cuadrática completa de la forma $ax^2 + bx + c = 0$ tienen un interés importante los coeficientes a, b y c y las raíces de la ecuación x_1 y x_2. La formación de la ecuación se basa en dos conceptos fundamentales: la *suma* y el *producto* de las raíces.
La suma de las raíces de una ecuación completa de segundo grado es igual al coeficiente del segundo término cambiado de signo, dividido por el coeficiente del primer término. El producto de las raíces de una ecuación completa de segundo grado, es igual al término independiente dividido por el coeficiente del primer término. En ambos casos influirá el valor del discriminante $D = b^2 + 4ac$ si $D > 0,\ D = 0$ ó $D < 0$.
Los antiguos egipcios, utilizando fracciones unitarias o egipcias, habrían resuelto la ecuación de la siguiente forma:
Sean m y n las raíces de la ecuación, entonces, tomando inversos resolvían:

$$\frac{1}{m} + \frac{1}{n} = \frac{Q}{Q+1} \text{ de donde } Q = \frac{m+n}{mn-(m+n)} = \frac{S}{P-S} = \frac{b}{c-b}$$

La ecuación generada es

$$x^2-(m+n)x+mn=(x-m)(x-n)$$

equivalente a $x^2-Sx+P=0$ y que escribimos como:

$$x^2-bx+c=0$$

Ecuación que admite las raíces:

$$x_1=m \text{ y } x_2=n$$

7.2.A partir de 28 generar una ecuación cuadrática.

Como en número $28=2^2\cdot 7$ podemos crear dos parejas: {2,14},{4,7}.

Tomamos la segunda por estar más centrada al número original, y tenemos:

$$x^2-(4+7)x+4\cdot 7=(x-4)(x-7)$$

La ecuación $x^2-11x+28=0$ admite como soluciones $x_1=4$ y $x_2=7$.
Vamos a crear dos sistemas a partir de los coeficientes 11 y 28.
Para $x^2-11x+28\equiv 0(mód.11)$ la ecuación se simplifica a $x^2\equiv 5(mód.11)$. Esta ecuación tendrá solución si y sólo si 5 es resto cuadrático respecto a 11. Como $5^{(11-1)/2}\equiv 1(mód.11)$ confirma que sí es resto cuadrático, la ecuación tiene como soluciones $x^2\equiv 4,7(mód.11)$.
Para $x^2-11x+28\equiv 0(mód.28)$ la ecuación se simplifica a $x^2+17x=0(mód.28)$. Esta ecuación tendrá solución si a su vez la tiene con los módulos 2, 4 y 14.

Para $x^2+17x=0(mód.2)$ tiene como soluciones: $x=0,1(mód.2)$
Para $x^2+17x=0(mód.4)$ tiene como soluciones: $x=0,3(mód.4)$
Para $x^2+17x=0(mód.14)$ tiene como soluciones: $x=0,4,7,11(mód.14)$

Aplicando el Teorema Chino de Restos, obtenemos:

$$x=0,4,7,11(mód.28)$$

7.3. A partir de 17 generar una ecuación cuadrática.

El número 17 es primo por tanto, vamos a tomarlo como suma de números, por ejemplo {10,7}. La ecuación propuesta podría ser $x^2-17x+70=0$ que admite como soluciones 7 y 10.
Para la ecuación $x^2-17x+70\equiv 0(mód.17)$ que simplificamos a $x^2\equiv 15(mód.17)$, admite como raíces las primitivas 7 y 10.
Para la ecuación $x^2-17x+70\equiv 0(mód.70)$ que simplificamos a $x^2+53x\equiv 0(mód.70)$, admite como soluciones:

$$x\equiv 0,7,10,17,35,42,45,52(mód.70)$$

Vamos a considerar la resta de 10 y 7, de donde $x^2+3x-70=0$ que admite como raíces $x_1=7$ y $x_2=-10$.

Para la ecuación $x^2+3x-70\equiv 0(mód.3)$ que simplificamos a $x^2\equiv 1(mód.3)$, admite como raíces $x\equiv 1,2(mód.3)$.

Para la ecuación $x^2+3x-70\equiv 0(mód.70)$ que simplificamos a $x^2+3x\equiv 0(mód.70)$, admite como raíces:

$$x\equiv 0,7,25,32,35,42,60,67(mód.70)$$

7.4. A partir de 69 generar una ecuación cuadrática.

El número factoriza como $69=3\cdot 23$ por lo que podemos generar $x^2-26x+69=0$, que admite como raíces el 3 y el 23.

Para la ecuación $x^2-26x+69\equiv 0(mód.69)$ que simplificamos a $x^2+43x\equiv 0(mód.69)$, admite como raíces:

$$x\equiv 0,3,23,26(mód.69)$$

Para la ecuación $x^2+20x-69\equiv 0(mód.69)$ equivalente a $x^2+20x\equiv 0(mód.69)$, la solución sería $x\equiv 0,3,46,49(mód.69)$.

Para la ecuación $x^2+20x-69\equiv 0(mód.20)$ equivalente a $x^2\equiv 9(mód.20)$, tendrá solución si la tiene también con los módulos 2, 4 y 5.

Para $x^2\equiv 1(mód.2)$ admite la solución $x\equiv 1(mód.2)$
Para $x^2\equiv 1(mód.4)$ admite la solución $x\equiv 1,3(mód.4)$
Para $x^2\equiv 1(mód.5)$ admite la solución $x\equiv 2,3(mód.5)$

Y mediante el Teorema Chino de Restos, obtenemos:

$$x\equiv 3,7,13,17(mód.20)$$

7.5. A partir de 61 generar una ecuación cuadrática.

La raíz cuadrada de 61 está comprendida entre $8^2>61>7^2$. Supongamos que tomamos la diferencia $61-7^2=12=2^2\cdot 3$ y escribimos 61 como $7^2+3\cdot 2^2=61$. Vamos a tomar como ecuación generada $x^2-14x+61=0$ que tiene como solución, $x_1=7+2\sqrt{3}i$ y $x_2=7-2\sqrt{3}i$, dos raíces complejas. (*)

Para la ecuación $x^2-14x+61\equiv 0(mód.14)$ equivalente a $x^2\equiv 9(mód.14)$, admite como solución $x\equiv 3,11(mód.14)$.

Para la ecuación $x^2-14x+61\equiv 0(mód.61)$ equivalente a $x^2+47x\equiv 0(mód.61)$, admite como solución $x\equiv 0{,}14(mód.61)$.

(*) La ecuación viene generada por las soluciones previas, esto es, suma y producto de las mismas:

$$S=\left(7+2\sqrt{-3}\right)+\left(7-2\sqrt{-3}\right)=14 \text{ y } P=\left(7+2\sqrt{-3}\right)\cdot\left(7-2\sqrt{-3}\right)=61$$

6.8. Algunas Aplicaciones: Código ISBN

8.1. Códigos ISBN con 10 cifras

El **I**nternational **S**tandard **B**ook **N**umber (ISBN) es un identificador único para libros, creado para uso comercial. Se creó en el Reino Unido y alcanzó el rango de estándar internacional en 1970.

Hasta el año 2007, todas las ediciones y variaciones de un libro recibían un ISBN de 10 dígitos divididos en los siguientes cuatro grupos:

- Código de país o lengua de origen (ISBN por país)
- Código del editor, asignado por la Agencia Nacional del ISBN
- Número del artículo, elegido por el editor.
- Dígito de control.

El código de país es 0 ó 1 para países de habla inglesa, 2 para países de habla francesa, 3 para países de habla alemana, etc. El sistema original ISBN carecía del código de país, pero anteponiendo un 0 a un número ISBN de 9 dígitos se creaba un ISBN válido. El código de país puede tener hasta 5 dígitos de longitud.

El número del editor es asignado por la Agencia Nacional del ISBN, el número del artículo es elegido por el editor.

La clave del ISBN está en este dígito de control, concretamente en cómo se calcula dicho dígito. Dicho cálculo se realiza de la siguiente forma:

> Cuando se tienen ya todos los códigos de país, editor y artículo se colocan y multiplican por cada uno de los números de la posición que ocupan, es decir, el primero por 1, el segundo por 2, el tercero por 3 y así sucesivamente hasta el último que se multiplicará por 9. La suma resultante se divide por 11 para obtener un resto. Este resto, al que llamaremos r que tendrá un valor comprendido entre 0 y 10. Si r está entre 0 y 9, el dígito de control será r, si el resto es 10 el dígito de control será X.

8.2.Comprobar el código de control de ISBN: 84-935271-0-6.

Vamos a comprobar la autenticidad del código ISBN: 84-935271-0-6 que corresponde a la obra Análisis Matemático I (de una variable real), de Juan de Burgos Román, Catedrático de Matemática Aplicada, Escuela Superior de Ingenieros Aeronáuticos, Universidad Politécnica de Madrid.

ISBN	**8**	**4**	**9**	**3**	**5**	**2**	**7**	**1**	**0**	6
Multiplicar por	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	
Producto	*8*	*8*	*27*	*12*	*25*	*12*	*49*	*8*	*0*	**149**

Como $149 \equiv 6(mód.11)$, el código de control es 6 además, 84 es el código país que corresponde a España.

Como podrán comprobar, si tiene oportunidad para ello, el código de barras de este libro es:

8.3.Códigos ISBN con 13 cifras

La longitud del código ISBN pasó de 10 a 13 dígitos el 1 de enero de 2007. Desde entonces el ISBN está formado por 5 grupos en lugar de 4. Desde el año 2007 el ISBN va precedido por el número 978, que identifica el producto libro.

La forma de calcular el dígito de control es distinta al anterior. Lo que se hace es tomar los primeros 12 dígitos y multiplicar el primero por 1, el segundo por 3, el tercero por 1, el cuarto por 3 así sucesivamente hasta llegar al número 12, luego se suman todos los productos. A continuación esta suma se divide por 10 obteniendo un resto r. El dígito de control será $10-r$, si r es distinto a cero, o bien r si es cero.

8.4.Comprobar el código de control de ISBN: 13: 978-0-12-372487-8.

El número ISBN: 13: 978-0-12-372487-8 corresponde a la obra Elementary Number Theory with Aplications de Thomas Koshy, profesor de matemáticas en la Framingham State University de Boston.

ISBN	***9***	***7***	***8***	***0***	***1***	***2***	***3***	***7***	***2***	***4***	**8**	**7**	8
Multiplicar por	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	1	3	
Producto	*9*	*21*	*8*	*0*	*1*	*6*	*3*	*21*	*2*	*12*	8	21	**112**

Como $112 \equiv 2(mód.10)$ donde $r=2$, el dígito de control es $10-2=8$ además, el cero denota la procedencia de Estados Unidos.

Como en el caso anterior, el código de barras generado para este libro es:

8.5.Crear un ISBN para estos apuntes.

Si estos apuntes vieran la luz, sería en España e iría precedido del número 978 seguido del 84 como código de país y le agregaríamos 1712939. El número resultante sería 978-84-17-12919 al que habría que añadir el dígito de control. Calculamos dicho dígito de la manera siguiente:

ISBN	***9***	***7***	***8***	***8***	***4***	***1***	***7***	***1***	***2***	***9***	**3**	**9**	2
Multiplicar por	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	*1*	*3*	1	3	
Producto	*9*	*21*	*8*	*24*	*4*	*3*	*7*	*3*	*2*	*27*	3	27	**138**

Como $138 \equiv 8(mód.10)$ donde $r = 8$, el dígito de control es $10 - 8 = 2$ además, el 84 denota la procedencia española. El número ISBN: 978-84-17-12939-2, hipotéticamente, corresponde la obra *Aritmética Modular, Un Paseo a Través de los Números.*
El código de barras generado para este libro sería:

BIBLIOGRAFIA:
APOSTOL, Tom M., Cálculus Tomo I, ISBN: 84-291-5002-1
BURGOS ROMÁN, Juan de, Análisis Matemático I, ISBN: 84-935271-0-6
CORTÁZAR, Juan, Tratado de Álgebra Superior, Edición 1858
CRANTZ, Paul, Aritmética y Álgebra, Edición 1926
EDWARDS, Harold M., Galois Theory, ISBN: 0-38790-980-X
KOSHY, Thomas, Elementary Number Theory with Aplications, ISBN: 978-0-12-372487-8
PHILLIPS, BUTTS y SHAUGHNESSY, Álgebra con Aplicaciones, ISBN: 968-6034-93-5
SWOKOWSKI y COLE, Álgebra y Trigonometría con Geometría Analítica, ISBN: 968-7529-26-1
TATTERSALL, James T., Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0

APOYO INTERNET
http://es.wikipedia.org/wiki/Ecuaci%C3%B3n_de_segundo_grado
http://maralboran.org/wikipedia/index.php/Ecuaciones_de_segundo_grado#Ecuaciones_de_segundo_grado_incompletas
http://thales.cica.es/rd/Recursos/rd99/ed99-0161-02/ed99-0161-02.html
http://www.akiti.ca/Mathfxns.html (Solución de ecuaciones)
http://www.sectormatematica.cl/educmedia.htm
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Programa matemático)
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Soluciones Ruffini)
http://www.vadenumeros.es/tercero/ecuaciones-de-segundo-grado.htm
http://www.vitutor.com/ecuaciones/2/ecu_Contenidos.html
http://www.wolframalpha.com/examples/ (Programa matemático)
http://www.wolframalpha.com/examples/ (Soluciones algebraicas)

ISBN: APOYO INTERNET
http://barcode.tec-it.com/barcode-generator.aspx?LANG=es (Códigos de barra)
http://en.wikipedia.org/wiki/International_Standard_Book_Number
http://es.wikipedia.org/wiki/ISBN
http://www.barcoderobot.com/isbn-13/9788417129392/ (Generador del dígito de control)
http://www.mcu.es/libro/CE/AgenciaISBN/InfGeneral/ISBN13.html